

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)  
 Black iPhone Model: A1661, FCC ID: BCG-E3087A, IC:  
 579C-E9087A, Currently in DEA Possession

Case No.

1:18MJ-129

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Southern District of Ohio (identify the person or describe property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B

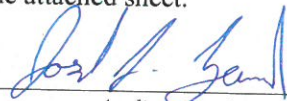
The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 21 U.S.C. § 841(a)(1) & 846, and the application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.  
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

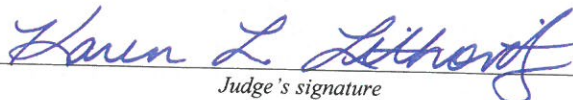
Joseph Zevchek, Special Agent, DEA

Printed name and title

Sworn to before me and signed in my presence.

Date:

2/26/18



Judge's signature

City and state: Cincinnati, Ohio

Honorable Karen L. Litkovitz, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO  
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF  
CELLULAR TELEPHONE DESCRIBED  
AS:

Black iPhone Model: A1661, FCC ID: BCG-  
E3087A, IC: 579C-E9087A, Currently in  
DEA Possession.

CASE NO.

1:18MJ-129

UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE

I, Joseph Zevchek, a Special Agent with the DEA, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Drug Enforcement Administration (“DEA”) and have been so employed since approximately October 2015. As such, I am an “investigative or law enforcement officer” within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

3. I am currently assigned to the DEA Cincinnati Resident Office. My official duties include the investigation of drug trafficking organizations and violations of federal narcotics laws, including offenses defined by 21 U.S.C. §§ 841, 843, and 846.

4. I have received training in and have experience investigating violations of federal narcotics laws including, but not limited to, Title 21, United States Code, Sections 841, 843, and 846. I have participated in numerous investigations involving a variety of investigative techniques, including physical and electronic surveillance methods; controlled purchases and deliveries of narcotics; the analysis of a wide variety of records and data, including pen register and trap and trace data as well as cell phone location data; and the debriefing of defendants, informants, and witnesses, as well as others who have knowledge of the distribution, transportation, storage, and importation of controlled substances. In addition, I have received specialized training in Title III investigations and have participated in several Title III investigations as a case agent, co-case agent, monitor, and surveillance agent.

5. Through these investigations, my training and experience, and conversations with other law enforcement officers, I have become familiar with the methods used by narcotics traffickers to distribute, transport, store, import, and safeguard controlled substances. I know that narcotics trafficking organizations have developed a number of methods to insulate their illegal activities from law enforcement detection. For instance, I know that members of narcotics trafficking organizations routinely utilize electronic communications facilities, including cellular telephones, to communicate operational directives and information concerning the conduct of the organization's illegal activities to other organization members; that organization members routinely use coded references in an effort to avoid law enforcement detection; that cell phones are often purchased through prepaid accounts using false identities to thwart the use of



subpoenas to identify members of the organization; and that the communication of time-sensitive information is critical to the successful conduct of these organizations' illegal activities. I am also familiar with narcotics traffickers' use of prepaid cellular and cellular phones, normal land line phones, public phones, debit calling cards, counter-surveillance, and the use of false and/or fictitious identities. Finally, I am familiar with the coded language used by narcotics traffickers during conversations in an attempt to disguise the true meaning of their conversations.

6. This affidavit is made in support of an application for a warrant to search the telephone, further described in Attachment A, for evidence and instrumentalities described further in Attachment B, concerning narcotics offenses, in violation of Title 21, United States Code, Sections 841 and 846.

7. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1) and 846, are located within the **Subject Phone**.

#### **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

8. The property to be searched is a **Black iPhone, Model: A1661, FCC ID: BCG-E3087A, IC: 579C-E9087A**, hereinafter the "Device." The Device is currently in DEA possession.

9. The applied-for warrant would authorize the forensic examination of this Device for the purpose of identifying electronically stored data particularly described in Attachment B.

**PROBABLE CAUSE**

10. The DEA has been investigating Manuel LARA, and the LARA Drug Trafficking Organization (“DTO”) for the purchase, sale, and distribution of methamphetamine and cocaine through Illinois and Ohio. As part of this investigation, the DEA has obtained several court-authorized wiretaps on LARA’s phones, and on the phone of a co-conspirator. On February 2, 2018, Acting Chief Judge Amy J. St. Eve of the United States District Court for the Northern District of Illinois signed an order authorizing Title III interceptions of wire and electronic communications to and from the telephone number 847-508-8799 (“Target Phone 4”) used by LARA.<sup>1</sup>

11. Generally, and as described in further detail below, as a result of interceptions over Target Phone 4, on February 13, 2018, law enforcement was able to identify and establish surveillance of a suspected narcotics transaction taking place in a Walmart parking lot in West Chester, Ohio, involving Carlos SERNA—a suspected courier in the LARA DTO—and an individual later identified as Jimmar LONG—a suspected distributor and purchaser of the LARA DTO’s narcotics. Law enforcement observed SERNA place a large box in a vehicle driven by LONG, who subsequently departed the parking lot in same vehicle. Law enforcement then attempted to initiate a traffic stop on LONG’s vehicle. Following a pursuit, during which LONG discarded the box from his vehicle (later found to contain four packages of suspect cocaine), LONG’s vehicle was stopped and LONG was taken into custody. A black iPhone with a clear case, bearing model number A1661, and FCC ID: BCG-E3087A (that is, the “**Subject Phone**”) was subsequently recovered from LONG’s vehicle. After securing the **Subject Phone**, law

---

<sup>1</sup> On July 25, September 25, and October 23, 2017, law enforcement obtained Title III interception orders for the number 224-407-1499 (“Target Phone 1”), used by LARA, from Chief Judge Ruben Castillo of the Northern District of Illinois, and intercepted many conversations over Target Phone 1 concerning the trafficking of drugs, including LARA’s conversations with his customers, suppliers, and couriers.

enforcement observed multiple calls come into the **Subject Phone** from a number used by LARA.

12. More specifically, on or about February 5, 2018, between approximately 5:30 p.m. and 9:00 p.m.,<sup>2</sup> LARA, who was using Target Phone 4, had several telephone conversations with Carlos SERNA, who was using telephone number 224-210-7731 (SERNA Phone A).<sup>3</sup> During these calls, LARA and SERNA discussed plans for SERNA to travel from Illinois to Cincinnati, Ohio the next day to rent a house for a week and conduct business on LARA's behalf.<sup>4</sup>

13. For example, on or about February 5, 2018, at approximately 5:32 p.m., LARA,<sup>5</sup> who was using Target Phone 4, had a telephone conversation with Carlos SERNA,<sup>6</sup> who was using SERNA Phone A (TP4 Session 154). During the call, LARA asked SERNA, "Are you going to go down there or what?" SERNA replied, "Yes, for sure. I told you I will." LARA

---

<sup>2</sup> Times are reported in Central time and are based on information from a pen register installed on Target Phone 4.

<sup>3</sup> On and about February 6, 2018, Acting Chief Judge Amy J. St. Eve of the Northern District of Illinois authorized, among other things, the installation of a pen register and trap/trace device and the collection of location data for SERNA Phone A.

<sup>4</sup> Some of the recorded conversations intercepted through the court-authorized wiretaps have been summarized in this Affidavit. The summaries of the recorded conversations do not include all statements made or topics covered during the course of the recorded conversations. The recordings are in Spanish. I based the summaries and the language quoted from the recorded conversations on draft transcripts prepared by DEA personnel. At various points in the Affidavit, I also have indicated (sometimes in brackets) my interpretation of words and phrases used in the recorded conversations. My summaries and interpretations also are based on the context of the recorded conversations, events occurring before or after the recorded conversations, information received from confidential sources, my knowledge of the investigation as a whole, my training and experience, and the training and experience of other law enforcement officers involved in this investigation.

<sup>5</sup> Voice identification of LARA is based on the following: on or about May 10, 2017, at approximately 4:35 p.m., a DEA confidential source met with LARA near the 5800 block of West Diversey in Chicago, Illinois. The purpose of the meeting was to look at a Honda Ridgeline (Subject Vehicle 29) for sale that LARA ultimately purchased that day. Surveillance observed LARA communicating with the confidential source, which was consistent with the recording of the meeting. Identification of LARA is based on a comparison to LARA's driver's license photograph.

<sup>6</sup> Voice identification of SERNA is based on the following: The telephone number (221) 210-7731 is subscribed to Silvia Flores at 14 Joslyn Drive, Elgin, Illinois. According to public databases, in 2016, SERNA was associated with this address. Specifically, SERNA's credit records, vehicle records, utility records, and phone records listed the 14 Joslyn Drive residence.



then said, "But, I don't want you to go like that. How are you going to go like that?" SERNA answered, "I'm good, bro." LARA then said, "Yeah, but you are not on your five senses, you can fuck it up. And it's way too much to fuck it up." LARA then added, "That's why I'm telling you to get well so you can leave tomorrow morning." SERNA then stated, "I'll be good for tomorrow morning, I'm going to stop right now. I'll be good." LARA then said, "You should take an airplane flight and get there early." SERNA asked LARA, "So, do you want me to purchase it myself." LARA answered, "Yes, so in case you fuck it up, you pay extra." LARA and SERNA then discussed arrangements for SERNA to purchase a flight and to send LARA the bill.

14. On or about February 6, 2018, LARA, using Target Phone 4, sent a text to an unknown individual ("TXT4-130") which read "5132528615," that is, the number for SERNA Phone B.<sup>7</sup> On February 7, 2018, a DEA undercover agent placed a consensually-recorded ruse call to SERNA Phone B and identified the voice of the person using SERNA Phone B as SERNA.

15. Based on my training and experience, and the training and experience of other law enforcement officers involved in the investigation, and based on the context and the content of these conversations, I believe that LARA called SERNA to ask SERNA if SERNA planned to conduct a narcotics transaction the next day on LARA's behalf. SERNA said that he did. LARA expressed concern that SERNA may not be sober enough to handle the transaction competently, but SERNA assured LARA that he would. LARA then told SERNA that he wanted SERNA to purchase a plane ticket for the following morning to ensure that SERNA

---

<sup>7</sup> On and about February 8, 2018, Chief Judge Ruben Castillo of the Northern District of Illinois signed and authorized, among other things, the installation of a pen register and trap/trace device and the collection of location data for SERNA Phone B.

arrived at the transaction in time, to which SERNA agreed. LARA then asked SERNA to send LARA the bill for the plane ticket.

16. At approximately 5:34 p.m., (TP4 Session 155), LARA, who was using Target Phone 4, had a telephone conversation with SERNA, who was using SERNA Phone A. During the call, SERNA asked LARA, "To Cin, right?" LARA answered, "Yes, to Cin. Let me call the Gaby dude and I'll call you back. Don't buy it yet."

17. Based on my training and experience, and the training and experience of other law enforcement officers involved in the investigation, and based on the context and the content of these conversations, I believe SERNA called LARA to confirm that he should purchase the plane ticket for Cincinnati, Ohio. LARA told SERNA that in fact Cincinnati was the airport nearest the planned location for the meeting, but told SERNA he wanted to check with another individual involved in the transaction ("Gaby") before SERNA purchased the plane ticket.

18. On or about February 12, 2018, at approximately 7:50 p.m., LARA, using Target Phone 4, received a call from telephone number (513) 609-7196, which was used by Jimmar LONG (TP4 Session 507).<sup>8</sup> During that call, LARA stated, "He already out there but he doesn't have a car to take that shit." LARA continued, "I don't know if you want to go to the crib." LONG responded, "Yeah." LARA stated, "Let me get it. Are you going?" LONG said, "Yeah." LARA then said, "Okay, let me ask him for the address." [LARA informed LONG that LARA would contact SERNA and ask for the address where SERNA was staying.]

---

<sup>8</sup> LONG was arrested by Ohio law enforcement on August 22, 2017, on a state charge for being a felon in possession of a firearm. According to Hamilton County, Ohio records, LONG was convicted and, on December 26, 2017, was released under probation. Law enforcement has reviewed recordings of multiple phone calls made by LONG during his incarceration and have confirmed, based on voice comparison, that the person using the 7196 phone number was LONG.



19. On February 13, 2018, at approximately 10:27 a.m., LARA, using Target Phone 4, placed a call to SERNA Phone A, utilized by SERNA (TP4 Session 518). During that call, LARA stated, "Send me an address of the Walmart to see what that guy says, if not, you will have to go more that way." SERNA responded, "I will send it to you shortly." [LARA asked SERNA to send LARA the address of a Walmart where SERNA and LONG could meet so that LARA could pass that information along to LONG.]

20. At approximately 11:01 a.m., LARA, using Target Phone 4, placed an outgoing call to SERNA Phone A, utilized by SERNA (TP4 Session 520). During that call, LARA asked, "You left already, right?" SERNA responded, "Yes, I am on my way. I am leaving the house right now." LARA informed SERNA, "He is five minutes away, bro."

21. At approximately 11:17 a.m., law enforcement received location data for SERNA Phone B placing SERNA at the Walmart supercenter at 8288 Cincinnati Dayton Rd, West Chester, Ohio.

22. At approximately 11:23 a.m., law enforcement located SERNA<sup>9</sup> sitting in a Walmart parking lot in a Honda sedan bearing Ohio temporary registration E822897 and utilizing a cellular telephone.

23. At approximately 11:25 a.m., law enforcement observed a black Lexus four door bearing Ohio registration HHF9410 moving slowly through the parking lot of the Walmart. At the same time, law enforcement observed SERNA moving through the parking lot in the Honda; both vehicles traveled to the front of the Walmart store and continued to move in the parking lot in tandem.

---

<sup>9</sup> Law enforcement was able to identify SERNA based on a comparison of the person seen by surveillance to known photographs of SERNA.

24. At approximately 11:28 a.m., both vehicles parked side by side on the west side of the Walmart in the parking lot of a gym. Law enforcement then observed SERNA exit the Honda wearing black sweat pants and a white t-shirt with a baseball hat, carrying a large white box and open the back driver's side passenger door of the black Lexus and placed the box into the vehicle. SERNA then proceeded to close the door and returned to the Honda and departed the area.

25. At approximately 11:30 a.m., the black 2006 Lexus departed the Walmart parking lot and traveled onto IR SB 75, exiting onto SR WB 126 (Ronald Reagan Highway). The black Lexus exited Ronald Reagan highway and traveled on SR SB 127 (Colerain Ave) turning onto W. Galbraith road, then onto Cheviot Road. At this time a Colerain Police officer operating a marked police car initiated a traffic stop of the black Lexus. The driver, later identified as Jimmar LONG, pulled over momentarily, and then accelerated. At that time, marked police cars from Colerain Police Department, and the Ohio State Highway Patrol followed. In the vicinity of 5550 Cheviot Road, LONG discarded a box, which appeared to be the same box surveillance observed SERNA place into LONG's vehicle. Law enforcement recovered the discarded box and discovered within four bricks of what initial Hamilton County lab results have identified as cocaine.

26. The pursuit of LONG's vehicle continued. A tactical decision was made by a uniformed officer to deploy stop sticks, which took effect and deflated LONG's tires causing LONG to lose control of the black Lexus and allowing officers to place LONG into custody.

27. During a subsequent search, law enforcement uncovered the **Subject Phone** in the driver's seat of LONG's vehicle.

28. While in law enforcement's possession, law enforcement observed multiple calls made to the **Subject Phone** from the phone number 708-209-0658 (LARA Phone A),<sup>10</sup> which law enforcement has previously identified as used by LARA. Specifically, based on toll analysis, LARA Phone A was in contact with the **Subject Phone** eight times between 12:18 p.m. and 1:01 p.m. Additionally, based on toll analysis, on that same day, Target Phone 4, also used by LARA, was in contact with the **Subject Phone** at approximately 1:05 p.m.

29. Since the time of LONG's arrest, February 13, 2018, the above-described **Subject Phone** has been in the government's custody.

30. At the time of arrest, data stored on the **Subject Phone**, including text and voice mail messages sent and received by the defendants during the course of the commission of the narcotics offenses, were not known.

31. The Device is currently in the lawful possession of the DEA. It came into the DEA possession following the arrest of Jimmar LONG.

32. The Device is currently in storage at the Cincinnati DEA Office. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the DEA.

#### ADDITIONAL INFORMATION

33. Based upon my training and experience, I know that cellular phones may contain relevant evidence of the narcotics offenses, including text messages made or received from the **Subject Phone** that are located in the memory of the **Subject Phone**, which messages may provide information regarding the identities of, and the methods and means of operation and

---

<sup>10</sup> LARA Phone A has been identified as an additional phone used by LARA based on common call analysis of other phones known to be used by LARA. On and about February 8, 2018, Chief Judge Ruben Castillo of the Northern District of Illinois signed and authorized the installation of a pen register and trap/trace device for LARA Phone A.



communication used by, the participants in the narcotics offenses. Moreover, digital photographs located in the memory of the **Subject Phone** may contain images of the tools or participants involved in the narcotics offenses. Moreover, digital photographs stored in the **Subject Phone** may contain images of the user of the **Subject Phone**, the user's associates (including persons involved in or knowledgeable about the subject offenses), places frequented by the user of the phone leading up to and during the subject offenses, and locations and instrumentalities used in committing the subject offenses.

34. In addition, based on my training and experience, I know that information stored within a cellular phone may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored within a cell phone can indicate who has used or controlled the cell phone. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, contacts lists, instant messaging logs, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the cell phone at a relevant time. Further, such stored electronic data can show how and when the cell phone and its related account were accessed or used. Such “timeline” information allows investigators to understand the chronological context of cell phone access, use, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the cell phone account owner.

35. Additionally, information stored within a cell phone may indicate the geographic location of the cell phone and user at a particular time (*e.g.*, location integrated into an image or

video sent via email or text message to include both metadata and the physical location displayed in an image or video). Stored electronic data may also provide relevant insight into the cell phone owner's state of mind as it relates to the offense under investigation. For example, information in the cell phone may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement). Unless this data is destroyed, by breaking the cell phone itself or by a program that deletes or over-writes the data contained within the cell phone, such data will remain stored within the cell phone indefinitely.

36. Through experience as a law enforcement officer and through the experience of other law enforcement officers as conveyed to me, I have learned that individuals involved in criminal offenses, including conspiracies to possess and distribute narcotics, commonly use cellular telephones as a means to communicate. Indeed, in this case, it appears that, at the least, LONG and LARA and LARA and SERNA were in communication in an effort to coordinate the narcotics transaction. Individuals involved in criminal offenses including conspiracies to possess and distribute narcotics, also often store telephone numbers and names or nicknames of fellow conspirators on their telephones and the telephones also reflect recent call history. Finally, individuals often use text messaging and digital photographs in furtherance of their criminal activity that are stored on cellular telephones. Because, as explained above, the **Subject Phone** is associated with the target(s) in this case, because there was telephonic communication between participants involved in the narcotics offenses, and because, in my experience and in the experience of other agents, defendants use telephones to contact co-conspirators, there is probable cause to believe the **Subject Phone**, described further in Attachment A, contain evidence of violations of narcotics.

**SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA**

37. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (*e.g.* computer hardware, computer software, computer-related documentation, and cellular telephones) to be processed later by a qualified computer expert in a laboratory or other controlled environment.

This is almost always true because of the following:

- a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.
- b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

38. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).



39. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain contraband or were used to carry out criminal activity.

**PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA**

40. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

41. The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

42. The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

### **TECHNICAL TERMS**

43. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an



extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

44. Based on my training, experience, and research, I know that these type of Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media

player, and a GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

45. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

46. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of these Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

47. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

### **CONCLUSION**

48. Based on the above information, I respectfully submit that there is probable cause to believe that narcotics offenses, in violation of Title 21, United States Code, Sections 841 and 846, have been committed, and that evidence and instrumentalities relating to this criminal conduct, as further described in Attachment B, will be found in Subject Phone, as further described

in Attachment A. I therefore respectfully request that this Court issue a search warrant for **Subject Phone** more particularly described in Attachment A, authorizing the seizure of items described in Attachment B, pursuant to protocol described in the addendum to Attachment B.

#### **REQUEST FOR DELAY OF NOTIFICATION**

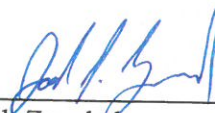
49. In accordance with 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), I further request that the warrant delay notification of the execution of the warrant for 30 days after the end of the authorized period of tracking (including any extensions thereof) because there is reasonable cause to believe that providing immediate notification may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice would seriously jeopardize the ongoing investigation by prematurely revealing its existence and giving suspects an opportunity to flee from prosecution, destroy or tamper with evidence, intimidate potential witnesses, notify confederates, and change patterns of behavior.

#### **REQUEST FOR SEALING**

50. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

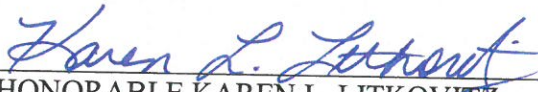


Respectfully submitted,



\_\_\_\_\_  
Joseph Zevchek  
Special Agent  
Drug Enforcement Administration

Subscribed and sworn to before me on this 26 day of February, 2018

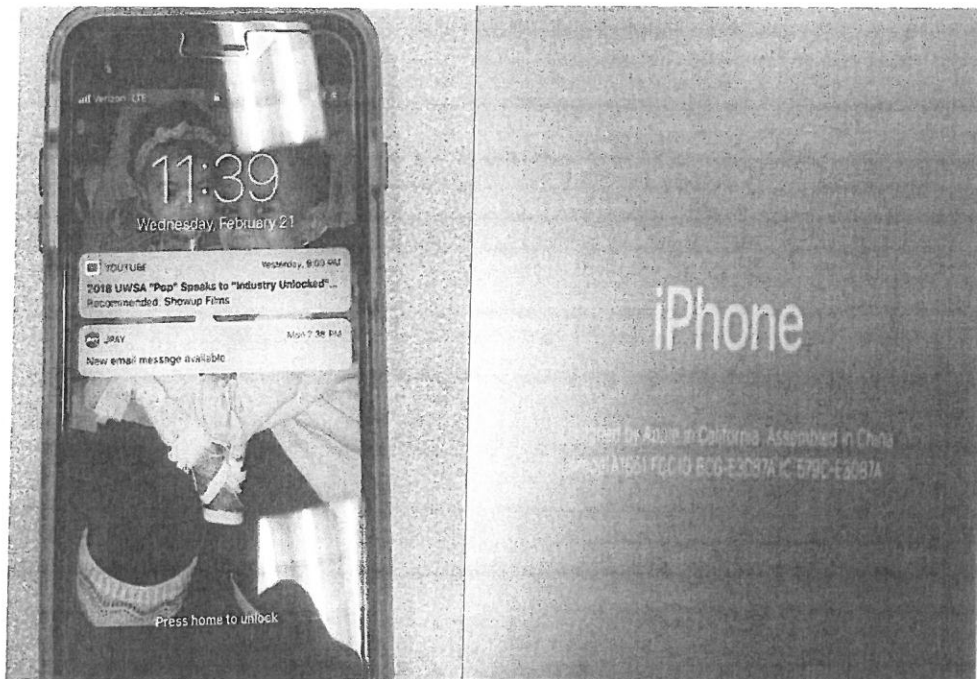


\_\_\_\_\_  
HONORABLE KAREN L. LITKOVITZ  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**DESCRIPTION OF ITEM TO BE SEARCHED**

The black iPhone with a clear case, bearing model number A1661, and FCC ID: BCG-E3087A, depicted below, currently in DEA possession.



**ATTACHMENT B**

The Device is currently located at the Cincinnati, Ohio DEA office.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.



**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

Evidence and instrumentalities concerning violation of Title 21, United States Code, Sections 841(a)(1) and 846, as follows:

1. All stored names, aliases, and numbers.
2. All messages, including voicemail, text messages, and email messages, pertaining to narcotics and/or narcotics trafficking, and the identification of co-conspirators.
3. Logs of telephone calls and text messages.
4. All digital photographs and videos that contains images related to the proceeds of and/or participation in narcotics trafficking, and items related to when and where the photographs and videos were created and sent or received, and who created them.
5. Any information pertaining to the phone's locations, including any search information contained within navigational applications on the phone.
6. Any internet searches or history pertaining to narcotics or narcotics trafficking.
7. Any SIM card located within the phone that helps to identify the cellular telephone number associated with the phone.
8. Any other stored information relating to the planning and/or commission of narcotics trafficking activity.

**ADDENDUM TO ATTACHMENT B**

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and
- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.